Non-deterministic Two-Way Quantum Key Distribution using Coherent States

Won-Ho Kye*
The Korean Intellectual Property Office, Daejeon 302-701, Korea
(Dated: February 1, 2008)

We propose a non-deterministic two-way quantum key distribution in which the quantum correlation is established by transmitting the randomly polarized photon. We analyze the security of the proposed quantum key distribution against photon number splitting, impersonation, and Trojan horse attack and quantify the security bound against mean photon number of the coherent state pulse. Finally, we remark the characteristic features of the protocol.

PACS numbers: 03.67.-a,03.67.Dd,03.67.Hk

Quantum key distribution (QKD) [1, 2, 3] is to generate shared secret information between distant parties with negligible leakage of the information to an eavesdropper Eve. The security of QKD is based on the no-cloning theorem: Eve can not extract any information without introducing errors [3], while the security of the classical key distribution or cryptography is supported by the computational complexity of the underling mathematical problems [4]. Since the QKD by Bennent and Brassard (BB84) [1], there has been security proof [5] and theoretical proposals to enhance the security [6].

The Ping-Pong protocol (PP) proposed by Boström et al. [7] is the first two-way quantum key distribution based on entangled qubit. It is a conceptually new scheme in the sense that the key is generated by the round trip of the qubit, while in the conventional QKD it is done with single trip. With this trend, Lucamarini et al. [8] proposed the two-way protocol without entanglement by merging the peculiarities of BB84 and PP and recently, Kye et. al., proposed to the three-way QKD [9] to make the encoding possible with relatively dense coherent-state pulse. One of the interesting aspects of their protocol is to use the qubit with random polarization, while in the conventional protocol, predefined finite number of polarization states is used [1, 2, 3, 7, 8].

In the multi-way quantum key distribution [7, 8, 9], the fact that the final key is led by only one party which allows creating the key in deterministic way is considered as an advantage for the direct encoding. However in some cases the deterministic feature of QKD without dissipation of the qubit often provides Eve with the room to track the protocol easily [15, 16]. That is to say the deterministic feature can play a role of potential security hole in QKD.

In this paper, we propose a non-deterministic two-way QKD in which the quantum correlation is established by transmitting the randomly polarized photon. The initial random polarization $|\theta\rangle$ with arbitrary $\theta \in [0, \pi]$ is compensated by acting the unitary operator $U(-\theta)$ on the returning qubit and the net encoding information can be extracted from that. In addition, the non-deterministic feature comes from the N number of screening angle which is chosen by Alice at the initial stage of the protocol. The key is created only when the matching condition of the corresponding screening angles is satisfied and it plays important role in blocking up the impersonation and Trojan horse attack.

QKD using coherent-state pulse has received much attentions in regard to the practical implementation [3, 9, 11]. Since there is no phase reference outside Alice or Bob's lab, a coherent-state $|\sqrt{\mu}e^{i\theta}\rangle$ of mean photon number μ is effectively described by photon number eigenstate $|n\rangle$ with Poission distribution: $|\sqrt{\mu}\rangle = \exp(-\mu/2)\sqrt{\mu}^n/\sqrt{n!}|n\rangle$ [12]. As we shall see, our proposal has remarkable advantages for implementation using coherent-state pulse, because the protocol allows not only to transmit the relative dense coherent pulse but also to increase the raw key creation rate. Our protocol is described as follows:

Protocol:

(P.1) Alice and Bob initiate the protocol by announcing a set $S(N)$ which has N number of screening angles,

$$S(N) = \{\alpha_1, \cdots \alpha_N\}, \tag{1}$$

where $N \geq 2$ and the screening angle α_i is defined as $\alpha_i = i\pi/(N+1)$.

(P.2) Alice take arbitrary angle θ and chooses screening angle α_a and random screening factor $s \in \{0, 1\}$. She prepares the qubit:

$$|\theta + \delta_{0s}\alpha_a\rangle, \tag{2}$$

where $\delta_{pq} = 1$ for $p = q$ otherwise $\delta_{pq} = 0$. Alice occasionally takes θ with the probability c as a predefined value $\theta^* \in \{0, \pi/2\}$ which is called authentication angle. If $\theta = \theta^*$ then the protocol follows the authentication mode (A-Mode) else transmission mode (T-Mode).

(A-mode 1) Bob chooses a screening angle α_b. He acts $U((-1)^k\pi/4+\alpha_b)$ on the received qubit, where k is key bit. The qubit becomes

$$|\theta^* + (-1)^k\pi/4 + \delta_{0s}\alpha_a + \alpha_b\rangle, \tag{3}$$

The fraction $(1-t)$ of the photons in the qubit enter into the Bob's detector, where t is the transmission efficiency of Bob's detector. Bob records the outcome O_b in his detector.

(A-mode 2) After acting $U(-\theta^* + \delta_{1s}\alpha_a)$ on the returning qubit, Alice has the qubit $|(-1)^k\pi/4+\alpha_b+\alpha_b\rangle$. She measures the qubit and the outcome is recorded as O_a.

(A-mode 3) Alice declares the mode is A-mode, then Alice and Bob announce the chosen screening angles α_a and α_b, respectively. If the screening angles satisfy that

$$\alpha_a + \alpha_b = \pi, \tag{4}$$

then the qubit incoming to Bob's detector is $|\theta^* + (-1)^k\pi/4\rangle$. So the corresponding outcome O_b and encoded key k are correlated by

$$O_b = k \oplus (2\theta^*/\pi), \tag{5}$$

where $\oplus$ is the addition on mod 2 space. If the verification is failed, Alice and Bob immediately terminate the protocol and initiate the protocol form (P.1) later. If $\alpha_a + \alpha_b \neq \pi$ in above step Alice and Bob return (P.2).

(T-mode 1) Bob chooses a screening angle α_b. He acts $U((-1)^k\pi/4+\alpha_b)$ on the received qubit, where k is key bit. The qubit becomes

$$|\theta + (-1)^k\pi/4 + \delta_{0s}\alpha_a + \alpha_b\rangle. \tag{6}$$

Bob returns the qubit to Alice.

(T-mode 2) Alice acts $U(-\theta + \delta_{1s}\alpha_a)$ on the returning qubit and it becomes $|(-1)^k\pi/4 + \alpha_a + \alpha_b\rangle$. Alice measures the qubit and gets the outcome O_a.

(T-mode 3) Alice and Bob announce the chosen screening angles α_a and α_b respectively. If the screening angles satisfy that $\alpha_a+\alpha_b = \pi$, then Alice gets the key k for the outcome O_a:

$$O_a = k, \tag{7}$$

else Alice and Bob go to (P.2). If the desired key length is created then go to (P.3)

(P.3) Alice and Bob create key k_a and k_b by concatenating key bits and exchange the hash values $h(k_a)$ and $h(k_b)$ [9]. If $h(k_a) = h(k_b)$ then the key creation is finished else Alice and Bob start again from (P.1).

Eq. (5) shows Alice's integrity condition observed in Bob's detector(D0, D1 in Fig. 1), which plays an important role to detect lethal strategy like impersonation and Trojan Horse attack. Even though the key encoding is performed by Bob deterministically, the final key is rearranged whether the matching condition in Eq. (4) is satisfied or not. In the QKD the raw key creation rate depends on the number of screening angle and mode probability as

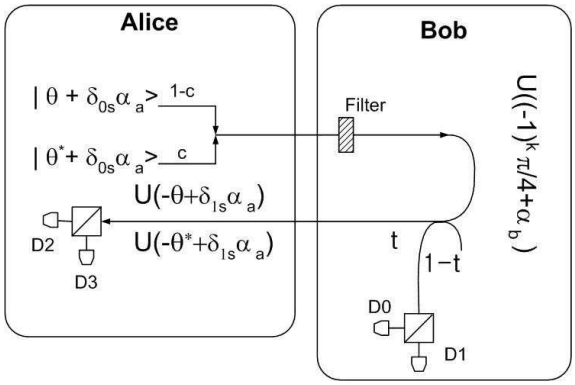

FIG. 1: Schematic diagram for the experimental setup. D0 and D1: Bob's detectors; D3 and D4: Alice's detectors; PBS: Polarization Beam Splitter. Bob has equipped the optical filter to reject undesired frequency.

$$R_{raw} = q\mu f_{rep} t_{link} \eta_{det}, \tag{8}$$

where q depends on implementation ($q = (1-c)/N$ for our protocol), f_{rep} is pulse rate, t_{link} the transmission and η_{det} the detection efficiency [3]. Now, we shall analyze the security of the protocol.

Security against photon number splitting (PNS) attack: Since A-mode is only for authenticating purpose, it is enough to consider that Eve's attack is focused on the T-mode in quantifying the PNS attack [10]. As usual, we assume that Eve is so superior that her action is limited only by the law of physics. Against the coherent state $|\sqrt{\mu}\rangle$ from Alice, she replaces the lossy channel by a perfect one and puts a beam splitter of transmission efficiency η in the middle [10]. The reflected field, which is a coherent state with its amplitude $|\sqrt{1-\eta}\sqrt{\mu}\rangle$, will be the source of information to Eve. In the protocol (T-mode.1)-(T-mode.3), the information transmitted between Alice and Bob is of random polarization. In our protocol, the photon polarizations lie on the equator of the Poincaré sphere. Thus, in this case, Eve's goal is to find the optimum state estimation from n qubits gives the maximal mean fidelity given by [17]:

$$I(n) = \frac{1}{2} + \frac{1}{2^{n+1}} \sum_{\ell=0}^{n-1} \sqrt{\binom{n}{\ell}\binom{n}{\ell+1}}. \tag{9}$$

Let us first consider the maximum information Eve can get from the Alice→ Bob channel in (a.2). The probability of there being n photons of the channel in the coherent

state $|\sqrt{(1-\eta)\mu}\rangle$ is $P_{AB}(n) = \exp[-(1-\eta)\mu]\frac{[(1-\eta)\mu]^n}{n!}$. The received qubit in Bob's end is $|\sqrt{\eta\mu}\rangle$ and after transmission of the detector, it becomes $|\sqrt{\eta t\mu}\rangle$. Thus in Bob → Alice channel, the probability of there being n photons in the coherent state $|\sqrt{1-\eta}\sqrt{\eta t\mu}\rangle$ is $P_{BA}(n) = \exp[-(1-\eta)\eta t\mu]\frac{[(1-\eta)\eta t\mu]^n}{n!}$

Then the maximum amount of information Eve can get from the channel in A→B and B→A is $I_{AB} = \sum_{n=0}^{\infty} P_{AB}(n)I(n)$ and $I_{BA} = \sum_{n=0}^{\infty} P_{BA}(n)I(n)$, respectively. The maximum information Eve can obtain is bounded by $I_E = \min(I_{AB}, I_{BA})$, which is plotted in Fig. 2 for various cases. Since the intensity of the coherent pulse decreases as the number of laps between Alice and Bob, I_E is actually determined by I_{BA}.

Now we define the critical value of initial amplitude α^* which gives the average number of photons delivered to Alice about 1 after (T-mode 3). Since the incoming amplitude of the coherent pulse in (T-mode 3) is $|\sqrt{(1-\eta)\eta t\mu}\rangle$, the critical value of initial amplitude is given by $\mu^* = 1/((1-\eta)\eta t)$. At the critical value of initial amplitude, maximum bound for Eve's information $I_E^* = \sum_{n=0}^{\infty} \frac{\exp(-1)}{n!} I(n) \approx 0.6900$, while the mutual information between Alice and Bob is unity (if the detector of Alice is not clicked in a particular time window due to the empty pulse, Alice and Bob could exclude the corresponding event by announcing that the pulse is empty). That is to say, at the critical amplitude Alice and Bob shares 31% higher information than that of Eve. So Alice and Bob could create the final key through the post processing like privacy amplification [18].

We remark the critical mean photon number in our protocol is on $5 \leq \mu^* \leq 15$ which is at least ten times larger value than $\mu \leq 0.2$ [13, 14] of conventional QKD. Accordingly, our protocol allow the higher raw key creation rate, even though the q factor in Eq. (9) is slightly smaller that the conventional QKD.

Security against Impersonation attack:

Eve can impersonate Bob to Alice and Bob to Alice in the quantum channel. This type of attack is effective on the protocol which transmits the qubit without dissipation of the qubit [7, 9]. Against our protocol, Eve may consider the following strategy:

(A1.1) After the step (P2) Eve intercepts the qubit and puts it in the quantum storage. Let's call it $E_1 = \{|\theta + \delta_{0s}\alpha_a\rangle\}$. Eve prepare fake qubit $|\theta' + \delta_{0s'}\alpha'_a\rangle$ and send it to Bob.

(A1.2) After the step (A-mode 1) or (T-mode1), Eve intercepts again the qubit whose state is given by $|(-1)^k\pi/4 + \theta' + \delta_{0s'}\alpha'_a + \alpha_b\rangle$. Eve gets the qubit $|(-1)^k\pi/4 + \alpha_b\rangle$ after acting $U(-\theta' - \delta_{0s'}\alpha'_a)$ on the qubit. Eve measures the qubit with guessing $\alpha_b = \alpha'_b$ and gets the outcome O_e and key $k' = O_e$.

(A1.3) Eve encodes the intercepted original qubit E_1 by acting $U((-1)^{k'}\pi/4 + \alpha'_b)$. The intercepted qubit becomes $E'_1 = \{|(-1)^{k'}\pi/4 + \theta + \delta_{0s}\alpha_a + \alpha'_b\rangle\}$. Eve sends the qubit to Alice.

If Eve impersonate the quantum channel during T-mode, the probability that Eve's guessing of α_b in (A1.2) was right is $1/N$. Accordingly Alice's key with Eve's impersonation includes the error with the probability and it should be noticed in the step (P.3).

On the other hand, if Eve impersonates the quantum channel during A-mode, Eve's impersonation can be also detected at the step (A-mode 3). In the step (A1.1), Eve's fake qubit $|\theta' + \alpha'_a\rangle$ is entered into Bob's detector with the transmission efficiency $(1-t)$. In that case, Eve's fake qubit violates with the integrity condition of Eq. (5) because the probability that Eve's guessing was matched with Alice's authentication angle as well as screening, $\theta' = \theta^*$ and $\alpha'_a = \alpha_a$ is almost null (here we use the fact that Eve does not know if the protocol in A-mode or T-mode). Eve's impersonation should be notice in the step (A-mode 3) with Eq. (5)-(6).

Security against Trojan Horse type attack:

Eve could attach ancillary qubit to the transmitted qubit and after the Bob's encoding, she reads out the encoding by measuring the ancillary qubit after separating out the ancillary qubit form the unified qubit. It is shown that the attack strategy is effective on the multiple-way protocol [7, 15]. We assume that Alice has a properly designed filter to reject the unnecessary of photons with split wave length as in Fig. 1 [3]. So Eve has some difficulty to distinguish ancillary form the full qubit and eventually she could not separate out the ancillary qubit form the unified qubit, perfectly. Nevertheless, to demonstrate the robustness of our protocol, we allow Eve to inject the ancillary qubit which has split wave length compared with the transmitted qubit and to separate the ancillary qubit from the returning qubit.

Eve may consider the strategy as follows:

(A2.1) After the step (A-mode 1) or (T-mode 1), Eve prepares an ancillary state $|0\rangle$ and attaches the ancillary onto the qubit from Alice. The qubit with the ancillary state is $|\theta + \delta_{0s}\alpha_a\rangle \otimes |0\rangle$. Eve sends the qubit to Bob.

(A2.2) After the step (A-mode 1) or (T-mode 1), the returning qubit becomes $|(-1)^k\pi/4 + \theta + \delta_{0s}\alpha_a + \alpha_b\rangle \otimes |(-1)^k\pi/4 + \alpha_b\rangle$. Eve separates out ancillary and keep the qubit in storage as $E_2 = \{|(-1)^k\pi/4 + \alpha_b\rangle\}$. After the step (A-mode 3) or (T-mode 3), Eve knows the Bob's screening angle α_b and measures the qubit in A_1 and reads the key k.

If Eve can distinguish if the protocol is in either T-mode or A-mode. Eve attacks on the protocol only when the protocol is in T-mode. In that case, she can read the key in the fraction of t of the created key, because the

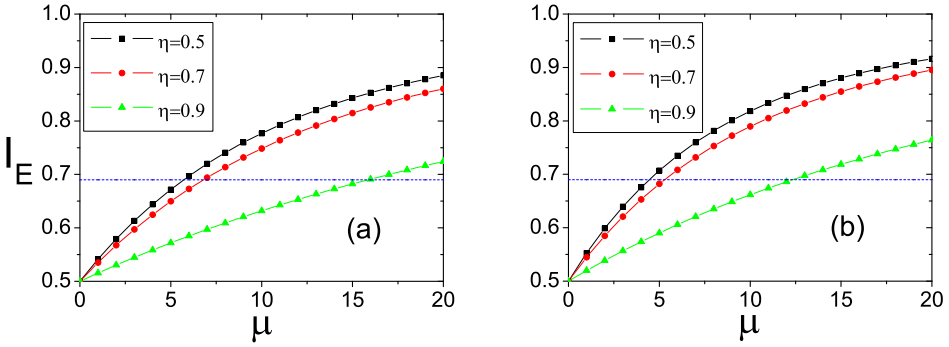

FIG. 2: Maximum bound for Eve's information I_E as a function of mean photon number μ of the coherent-state pulse according to various channel transmission efficiency η at the transmission efficiency of Bob's detectors $t = 0.7$ (a) and $t = 0.9$ (b). The horizontal line in (a) and (b) shows the maximum bound of information for Eve when Alice prepares the initial amplitude as the critical value $\mu = \mu^*$.

ancillary qubit sink into the Bob's detector with the fraction of $1 - t$. Unfortunately, there always exists θ which satisfies $\theta + \delta_{0s}\alpha_a = \theta^* + \delta_{0s'}\alpha'_a$, where $\alpha_a, \alpha'_a \in S(N)$ and $s, s' \in \{0, 1\}$ it inevitably induces the collision between two mode. Thus Eve can not distinguish the initial qubit state if it is in T-mode or A-mode unambiguously and she could not avoid to intervening during A-mode and her ancillary qubit sink into the Bob's detector. The ancillary qubit which does not carry the information Alice's screening angle and authentication angle makes the Bob's outcome O'_b violating the integrity condition. Thus Eve's Trojan Horse attack should be noticed in the step (A-mode 3).

CONCLUSIONS

We have proposed the non-deterministic two-way QKD protocol and have demonstrated the security of the proposed protocol against PNS, Impersonation and Torjan Horse attack. Finally, we emphasize that the proposed protocol has the following advantages compared with the conventional QKD. 1) The quantum correlation is established by exchanging the qubit with completely random polarization. For that reason, our protocol can be implemented with relatively dense coherent pulse. 2) Since the mean photon number μ can be safely set is much higher value than that of conventional QKD [13, 14] (see the last paragraph of PNS analysis), the corresponding raw key creation rate is higher than that of the conventional two-way QKD. 3) The protocol provides the tunable security depending on the number of screening angle N. Even if an eavesdropper try to know the current status of the protocol by a combination of photon number quantum non-demolition measurement[10] and unambiguous state discrimination [20], it can be avoided by increasing the number of screening angle N.

* Electronic address: whkyes@empal.com

[1] C. H. Bennet and G. Brassard, 1984, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, (IEEE, New York), pp.175-179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] B. Schneier, *Applied Cryptography*, Second Edition, (John Wiley, New York, 1996).
[5] P.W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[6] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X.-B. Wang, Phys. Rev. Lett. **94** 230503 (2005).
[7] K. Boström and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
[8] M. Lucamarini and S. Mancini, Phys. Rev. Lett. **94**, 140501 (2005).
[9] W.-H. Kye, C. Kim, M. S. Kim and Y.-J. Park, Phys. Rev. Lett. **95**, 040501 (2005).
[10] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[11] N.Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, quant-ph/0411022 (2004).
[12] K. Molmer, Phys. Rev. A **55**, 3195 (1997); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[13] D. Stucki et al., New Journal of Phys. **4**, 41.1-41.8 (2002).
[14] A. Acín, N. Gisin, and V. Scrani, Phys. Rev. A. **69**, 012309 (2004).

[15] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003); Q.-Y. Cai, Phys. Rev. Lett. **91**, 109801 (2003); H. Hoffmann, K. Boström, and T. Felbinger, quant-ph/0406115 (2004).
[16] Q. Zhang et al., Phys. Rev. Lett. **96**, 078901 (2006); Won-Ho Kye et al. Phys. Rev. Lett. **96**, 078902 (2006).
[17] R. Derka, V. Bužek and A. K. Ekert, Phys. Rev. Lett. 80, 1571 (1998).
[18] Bennett et al., "Generalized Privacy Amplification", IEEE Transactions on Information Theory, 1995.
[19] N. Gisin, S. Fasel, B. Kraus, H. Zbinden and G. Ribordy, quant-ph/0507063 (2005).
[20] M. Dušek, M. Jahma, and Norbert Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).